Lab 11

Hack the Box

Estimated time to complete: 50 Min

WHAT YOU WILL LEARN

How to create an account for Hack The Box, discover fun labs, connect to your remote hacking computer and walk you through your first lab

WHY IT'S IMPORTANT

Hack The Box allows you to learn and test your cybersecurity skills legally. Their free service provides you with your own attacker and target computer. With this site, you can continue to learn after you have completed all of the H.A.C.K labs and get more hands-on experience with real cybersecurity tools and techniques

SKILLS GAINED

- Connecting to Remote Machines
- Discovering Flags
- Utilizing a VPN

REQUIRED HARDWARE

- Raspberry Pi
- Internet Connection

DISCLAIMER: HACK THE BOX ALLOWS YOU TO PRACTICE YOUR HACKING SKILLS ON MACHINES THAT ARE MEANT TO BE HACKED. DO NOT ATTEMPT THESE LABS ON DEVICES OUTSIDE OF HACK THE BOX WITHOUT THE PERMISSION OF THE DEVICE OWNER.

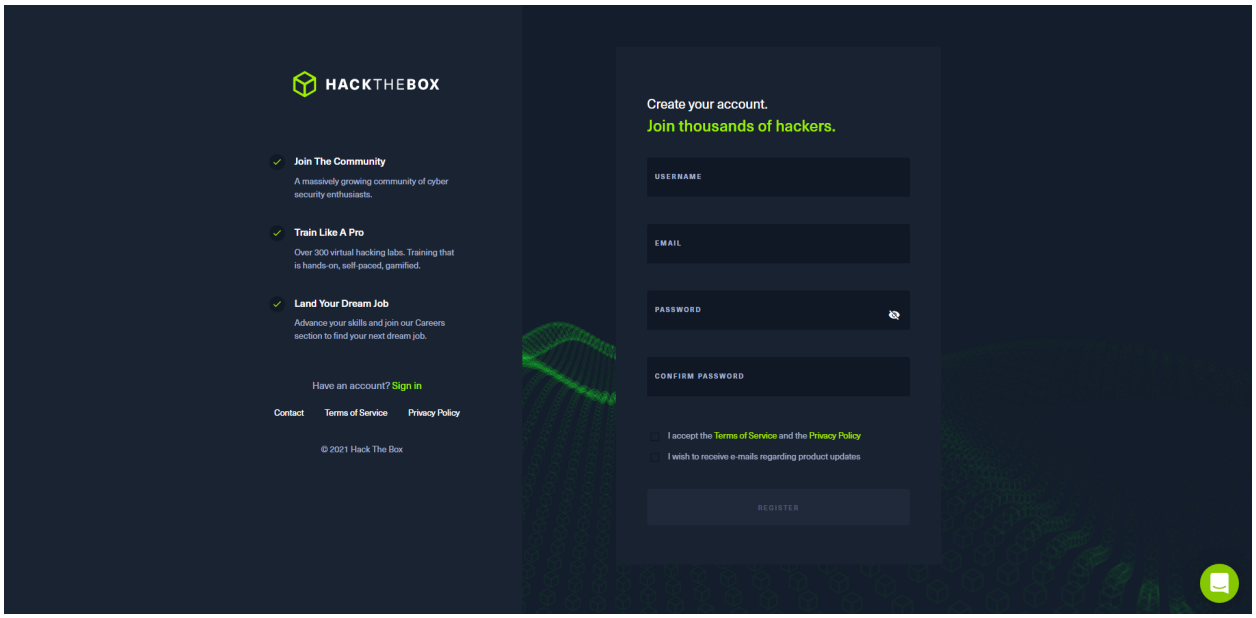
WHAT IS HACK THE BOX?

Hack The Box is an online site filled with hands-on hacking activities for various skill levels. The activities are designed to provide challenges through virtual machines to simulate real-world security issues in an intuitive environment. The two main categories on Hack the Box are split up between Boxes and Challenges. Boxes, or Machines, are vulnerable virtual machines hosted on Hack the Box's servers that can run different operating systems and have different sets of vulnerabilities. Challenges are small applications designed for different penetration testing techniques made to be attacked by the user. For each Box or Challenge you complete, you can earn points and rank up on the site.

MAKING AN ACCOUNT

To get started, we first need to create an account. Go to https://www.hackthebox.com/ and click "join now" to be redirected to a page where you can enter your username, email, and password. After filling out the page and clicking "register", you can click "skip onboarding" on the left side of the next page and you will be brought to Hack The Box's home page. There will be a banner at the top of the page stating that your email needs to be verified, so you can go ahead and do that now by opening the verification email and clicking "verify". This should redirect you back to Hack The Box to a page saying "Email Verified". If it doesn't automatically redirect you to

the dashboard, click on “Hack The Box” to get there.



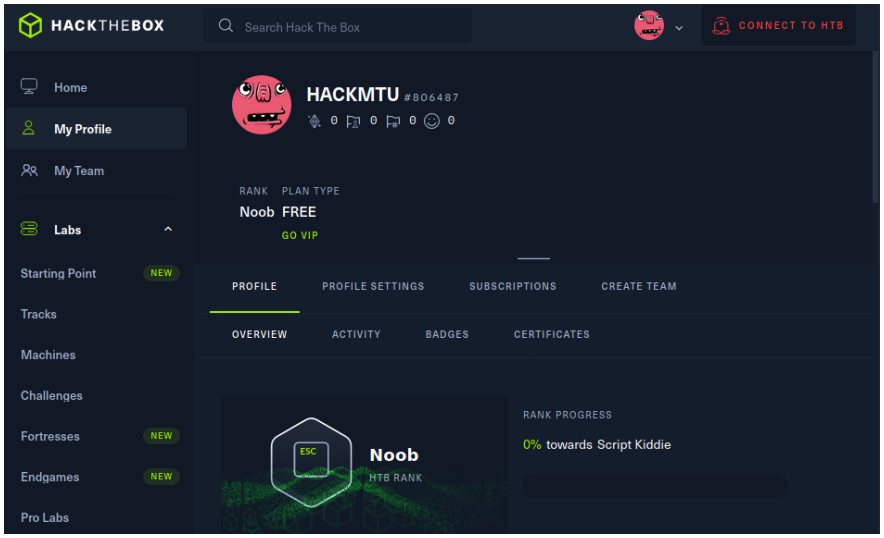
WHAT IS A VIRTUAL MACHINE?

Hack the Box utilizes virtual machines to create their lab environments. A virtual machine is a virtual environment that functions as its own computer system. A virtual machine has its own CPU, memory, storage, and network interface which are created on a physical machine. Software called a hypervisor is used when running a virtual machine. This allows the physical machine that the virtual machine is running on, also known as the host, to allocate resources from the hardware to provision them for use by the virtual machine. Virtual machines are very useful for having an isolated environment for testing various things that won’t interfere with the host environment. You can also use virtual machines to host multiple servers on one physical machine as they use small amounts of host resources.

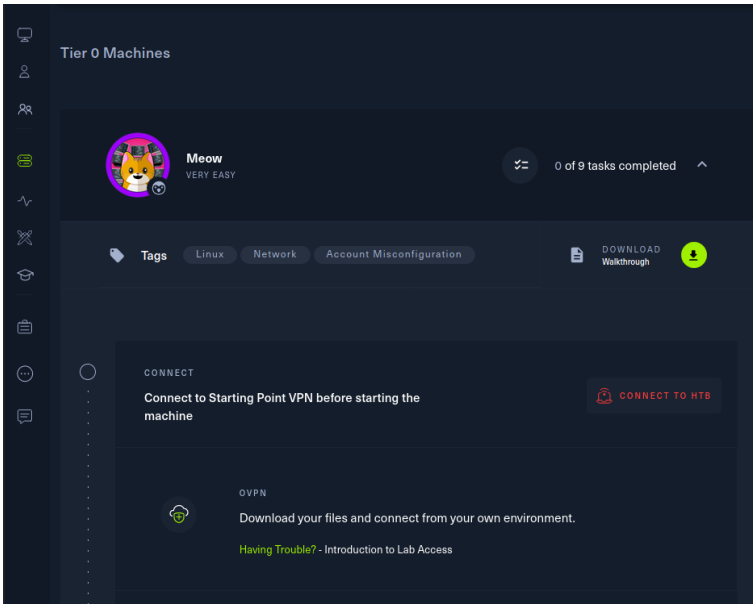
COMPLETING YOUR FIRST LAB

STEP 1: CONNECTING TO YOUR VIRTUAL MACHINE

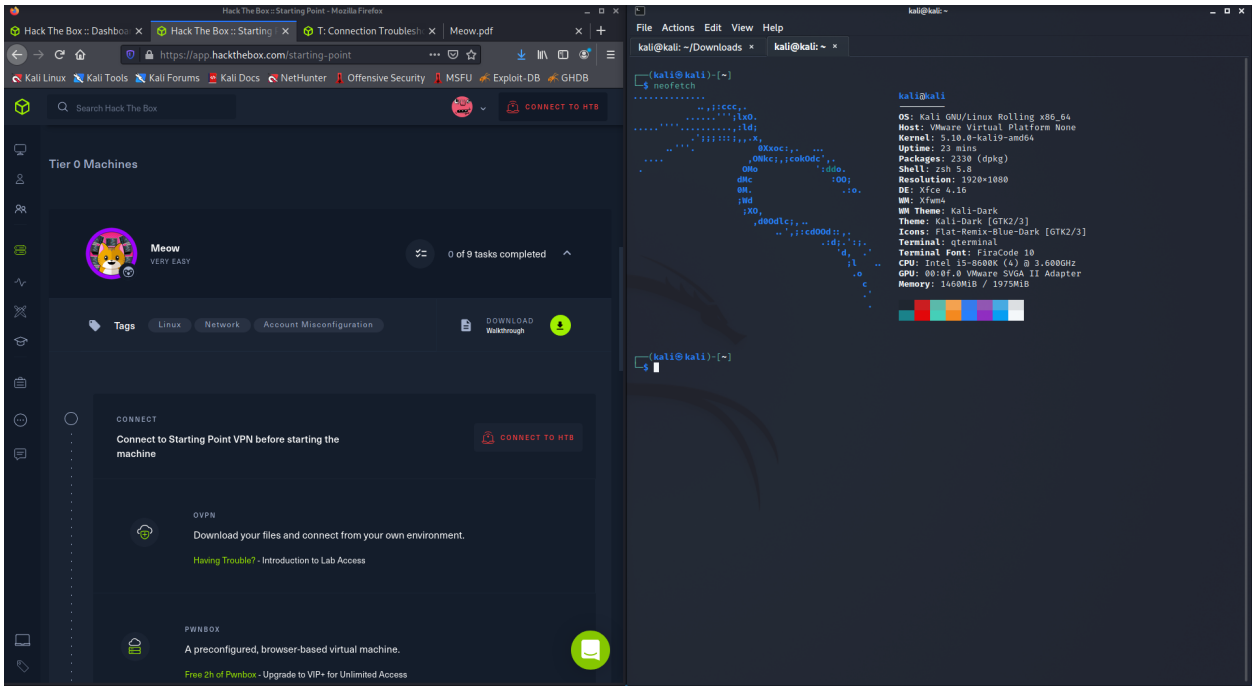
On the left side of the page, click on “Starting Point”



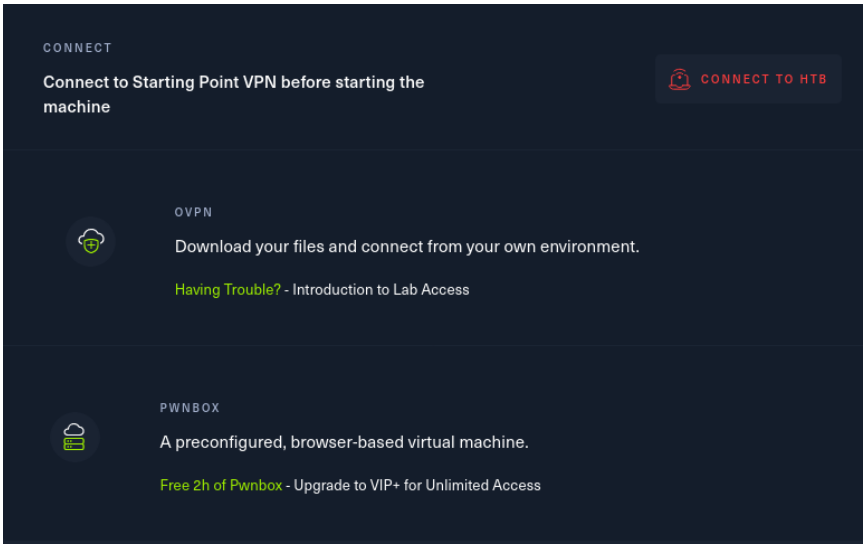
Scroll down and click on Meow - Very Easy under Tier 0 machines to get started. If you get stuck or need help, you can download the walkthrough in the top right of the HTB module.



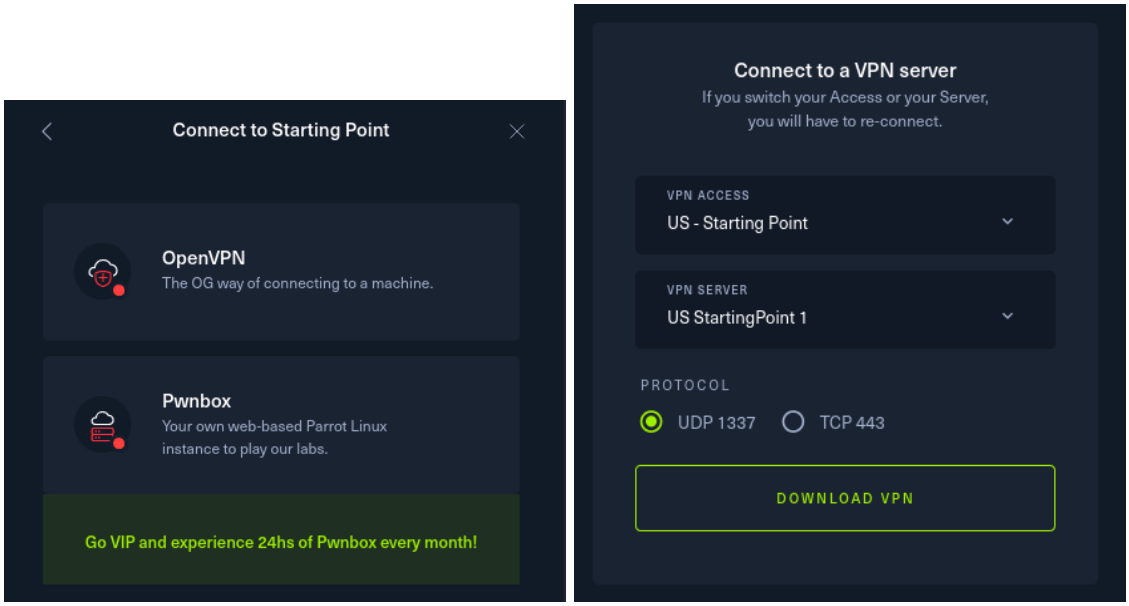
From this point on, we recommend you split your window to have HackTheBox on one side of your screen and a Kali terminal on the other, as this is how we plan to interact with our box.



Now we need to connect to the HackTheBox network using OpenVPN, this tool is preinstalled on Kali Linux. Click “Connect to HTB”.



Then click “OpenVPN”, change the protocol to UDP 1337, then click “Download VPN”, this will download a .ovpn file that will act as our configuration file for OpenVPN. Save the file.



In your Kali terminal, run **cd Downloads** to change to the Downloads folder and run the command **ls** to find your OpenVPN filename, the run the command:

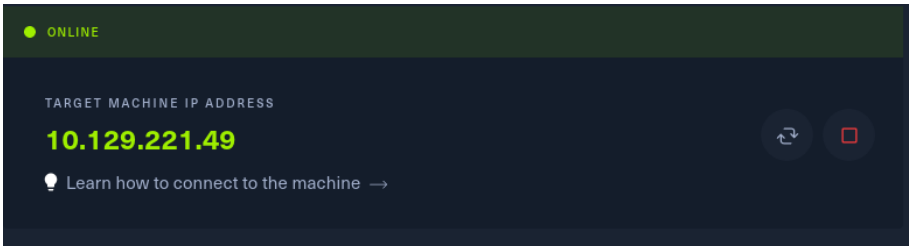
sudo openvpn starting_point_username.ovpn

The command should end with “Initialization Sequence Completed”, if the command doesn't work, make sure you are using the correct file name and are in the same directory as the file - You must now keep this terminal window open to maintain your VPN connection. (use Ctrl+Shift+T to open a new terminal window).

```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
starting_point_HACKMTU.ovpn

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn starting_point_HACKMTU.ovpn
2021-11-05 11:21:11 WARNING: Compression for receiving enabled. Compression has been used in the past to break encry
ption. Sent packets are not compressed unless "allow-compression yes" is also set.
2021-11-05 11:21:11 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-
128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers o
r change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2021-11-05 11:21:11 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEA
D] built on May 14 2021
2021-11-05 11:21:11 library versions: OpenSSL 1.1.1l  24 Aug 2021, LZO 2.10
2021-11-05 11:21:11 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentica
tion
2021-11-05 11:21:11 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentica
tion
```

Back on HackTheBox, you might have to refresh the page or click the connect to HTB button again to make the site realize you have an open connection. Next, click “Spawn Machine” and continue on with the lab by answering questions.

Once you spawn a machine, it will give you an IP address of that virtual machine that you can now interact with in your terminal.



Using our box’s IP address, we can ping it in our terminal to ensure we can connect to it.

STEP 2: GETTING INTO OUR TARGET DEVICE

We can then run nmap to find any open ports on the machine.

```
┌──(kali㉿kali)-[~]
└─$ ping 10.129.221.49
PING 10.129.221.49 (10.129.221.49) 56(84) bytes of data.
64 bytes from 10.129.221.49: icmp_seq=1 ttl=63 time=49.2 ms
64 bytes from 10.129.221.49: icmp_seq=2 ttl=63 time=50.1 ms
64 bytes from 10.129.221.49: icmp_seq=3 ttl=63 time=49.2 ms
64 bytes from 10.129.221.49: icmp_seq=4 ttl=63 time=49.5 ms
64 bytes from 10.129.221.49: icmp_seq=5 ttl=63 time=50.0 ms
^C
--- 10.129.221.49 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 49.178/49.589/50.135/0.388 ms

┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.129.221.49
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-05 11:43 EDT
Nmap scan report for 10.129.221.49
Host is up (0.051s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

From our tests we can see that our box is reachable and that it has a port open, port 23 or telnet. Let's try to connect to the box using telnet. Telnet is a remote connection tool that allows you to connect to a machine using the command line over the internet. While it is useful, the service as a whole is fairly insecure and should only be used for this lab.

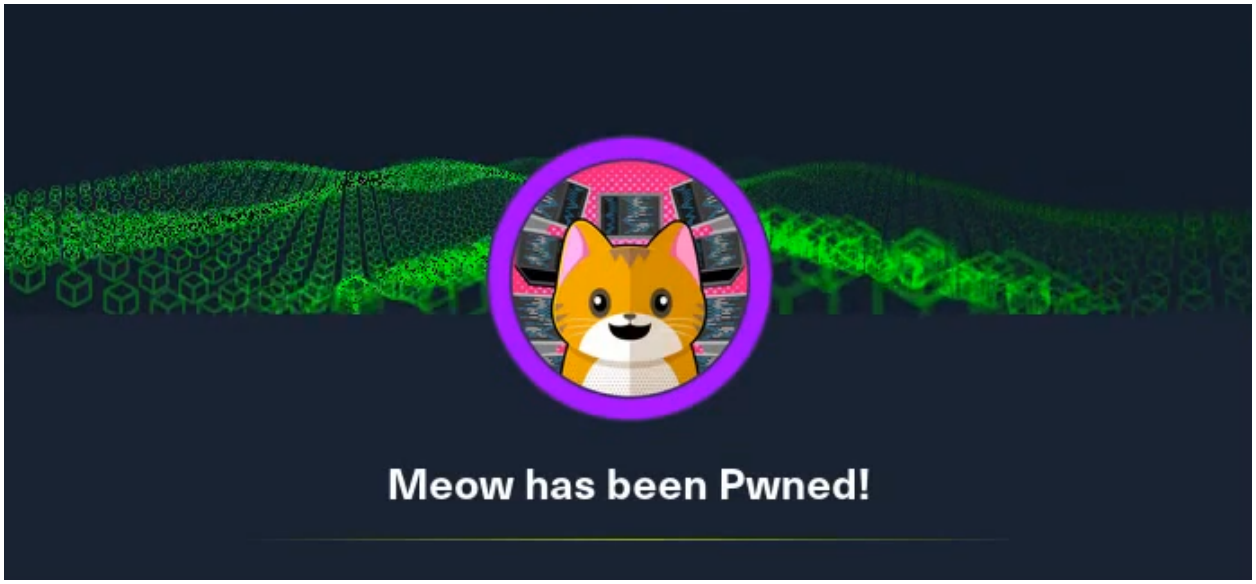
```
┌──(kali㉿kali)-[~]
└─$ telnet 10.129.221.49
Trying 10.129.221.49 ...
Connected to 10.129.221.49.
Escape character is '^]'.

Hack the Box
```

Log into the box with the account “root”, no password is required at this point in the lab.

```
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 05 Nov 2021 03:45:47 PM UTC

  System load:  0.0               Processes:             137
  Usage of /:   41.7% of 7.75GB   Users logged in:       0
  Memory usage: 4%                IPv4 address for eth0: 10.129.221.49
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
```

Run the **ls** command and you should see flag.txt in the current directory, this is the flag for the end of the lab, use the **cat** or **vim** command to view the flag and paste it into HTB (make sure to follow the format shown - "**HTB{flag}**".

Congrats! You just finished the first module!



EXERCISES:

For your final lab, you get to decide what exercises you want to do. There are numerous different boxes you can choose from. Pick 2 that interest you the most

REVIEW

1: What is the OS you use for Hack The Box Virtual Machine?

A) Windows

B) Parrot OS

C) Ubuntu

D) RedHat

2: Trying the hacking techniques learned in Hack The Box on devices outside the website is legal (True/False)

3: How many methods are there to connect to a Hack The Box Machine?

A) 1

B) 2

C) 3

D) 4

4: What VPN should you use to connect to a box?

A) NordVPN

B) ExpressVPN

C) Private Internet Access

D) OpenVPN

5: Hack The box allows you to check your points and can rank you against your friends. (True/False)

6: Which statement about Hack The Box is true?

A) You can get a certificate for completing some labs

B) Labs can be chosen based on difficulty

C) You can create a team with your friends to compete with or against each other

D) All of the above

Answers: 1:B 2:False 3:B 4:D 5:True 6:D